# Segment and Separate

## Objective

Segment and separate information based on sensitivity of information.

## Key Considerations

* [ ] Develop a target network security design that considers segmentation via network security zones, in alignment with [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38).
* [ ] Implement increased levels of protection for management interfaces.

## Validation

* [ ] Confirm that department has a target network architecture diagram with appropriate segmentation between network zones.

## Applicable Service Models

* IaaS, PaaS

## References

1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4
2. CSE Top 10 #5
3. Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)
4. Related security controls: AC‑4, SC‑7, SC‑7(5)